# APS Windows Servers

Steve Potempa

December 13, 2005

# Microsoft Windows Active Directory

- Authentication
  - User logon
  - VPN & Dial-up

- Group Policy
  - Configuration Control
  - Software Deployment

- The APS Windows domain was upgraded in October 2004 from a Windows NT 4 Domain.

- The XOR Windows domain
  - In service January 2004.
  - Provides authentication, file, and print services to beamline systems.
  - Provides a separate environment for beamline Windows systems, allowing for a different set of Group Policies and patch management philosophy.

# Cyber Security Related Activities

- Active Directory Group Policy is used to enforce configuration management of operating system and application settings for Windows 2000 and XP based systems.
    - This last shutdown the ISS network scans performed by IT reported zero Windows vulnerabilities on the public APS networks.

- Update Expert is used to remotely deploy Microsoft operating system and application patches and service packs.

# Cyber Security Related Activities (continued)

■ McAfee Virus Scan Enterprise 8i for desktop and server virus protection.

  – McAfee ePolicy Orchestrator to deploy and maintain Virus Scan.

  – Provides the capability to report and track virus activity.
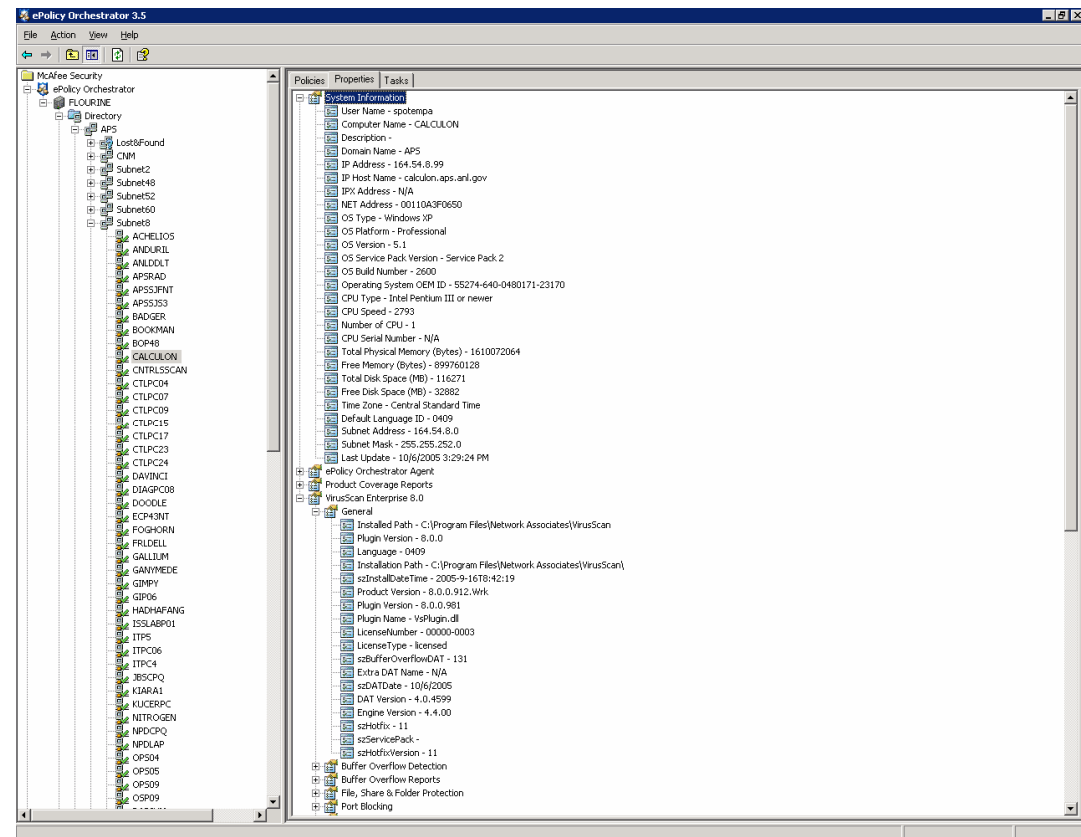
# Cyber Security Related Activities (continued)

■ Example of an immediate update due to the appearance of the 'R' variant of the Sober virus in the wild.

- Date: 2005-10-06 09:09:05
  - PCs at Current Virus Signature Version: 6
  - PCs with Out of Date Virus Signature Versions 546

- Date: 2005-10-06 10:28:52
  - PCs at Current Virus Signature Version: 549
  - PCs with Out of Date Virus Signature Versions: 10

## File & Print Services
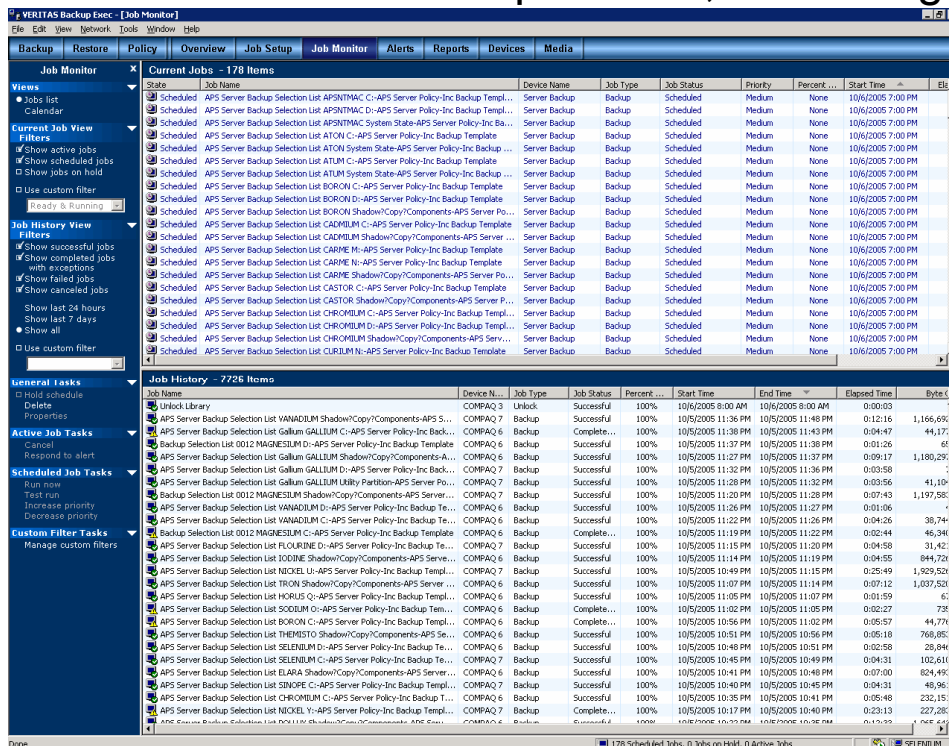
- User Home directories (z drive) .
- Central repository for Windows application installations.
- Print queues with the appropriate drivers that auto-install and update.

- Two node High Availability Windows cluster with ~2.5TB of disk.
  - Windows 2000 Cluster (January 2003).
  - Windows Server 2003 (December 2004).
  - 3rd node will be added to the Cluster during the Christmas shutdown.

## *Citrix Services*

- The Citrix servers provide access to Windows based applications and administrative applications (PARIS, AMOS, TMS, CMS, etc…).
  - Sun, Mac, Linux, and Windows based systems where conflicts with locally installed software occur (Pro/E).
  - Also provides remote access for the ASD Controls group to the Accelerator control systems via MEDM & Exceed.

- Secure remote web-based access to administrative and office applications via https://metis.aps.anl.gov.

- Windows Server 2003 & Citrix Metaframe XP
  - Three production servers – in service spring 2004.
  - Four supporting systems – Data store, Secure ticket authority, secure gateway, and web interface.
  - One test server – for testing patches and new software.

# *Backup Services*

- Data backup for all 32 Windows Servers and over 500 PC desktops.
  - Full backups occur weekly and incremental backups nightly.
- Six backup servers with five tape libraries process approximately 6TB a week.
  - The IT staff performs, on average, two restores per week.

## *Other Services*

- Microsoft Project Server
  - Used by ASD to coordinate Accelerator activities.

- Hewlett-Packard Web Jet Admin Server
  - Used to configure, secure, and report errors for HP printers.

- Vocera
  - Instant voice communications between users via the 802.11 wireless infrastructure.
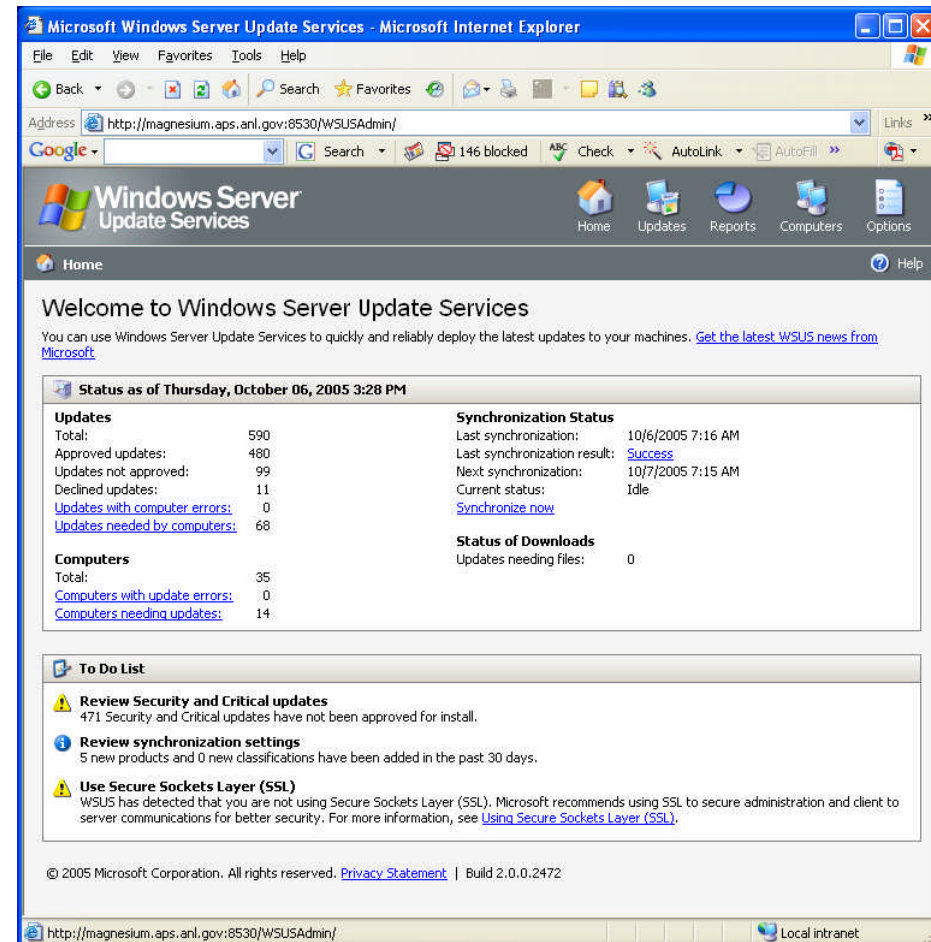
# The Future - Software Deployments with SpecOps Deploy

- **SpecOps Deploy addresses the short comings in Active Directory's Software deployment**
  - Scheduled and targeted deployments.
  - Feedback on how the deployment is proceeding.
  - Adds the ability to deploy traditional setup packages, such as Mozilla Firefox or Thunderbird.
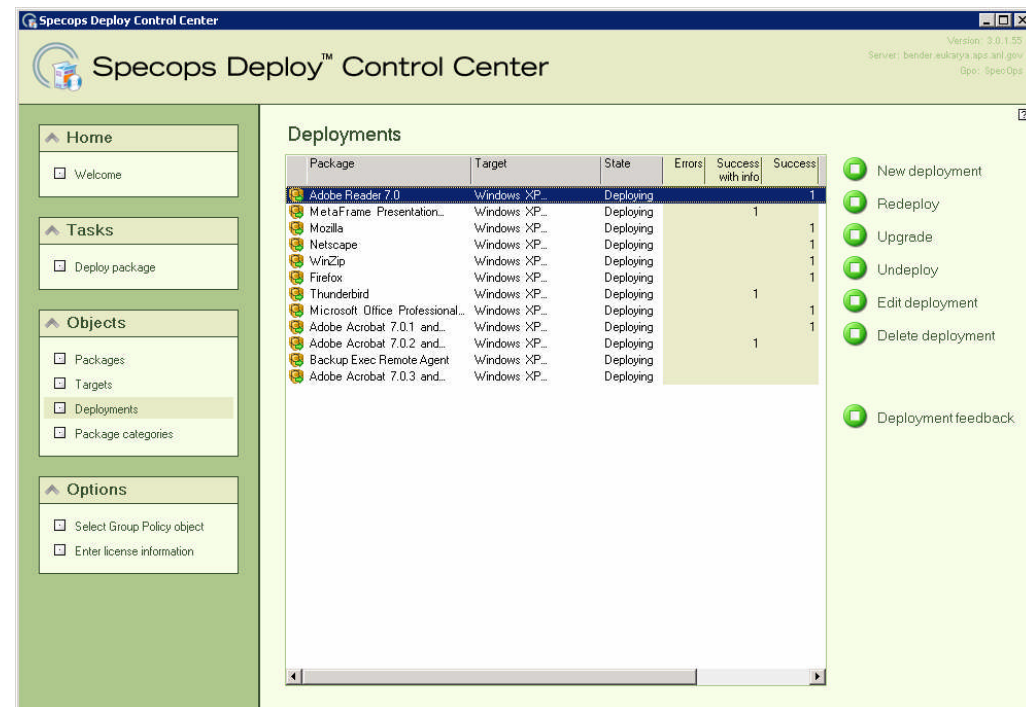
# The Future - Window Server Update Services (WSUS)

■ **More effective updates:**

– Update Expert is "push" based. Only the systems that are on-line will get the updates.

– WSUS is "pull" based. Systems will check-in with the WSUS server and will automatically download any required updates to the Windows operating systems or Microsoft Office applications.

– WSUS will provide an effective patch management for systems that are not continuously online, for example laptops.

# The Future – Software and Hardware Asset Inventory

- In February 2005 the IT group was required to complete an inventory of all Microsoft products for the Laboratory's Enterprise Agreement with Microsoft.
  - Some of the inventory collection process was automated.
  - All of the data correlation was done by hand.
  - This inventory will need to be repeated yearly for the duration of the Enterprise agreement.

- "Asset Tracking" by Opsware (formerly Asset Insight by Tangram) provides automated hardware and software inventory and reporting.